Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,502	01/19/2000	Cynthia Dwork	AM9-99-0138	3238

7590 09/11/2006

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/487,502
Filing Date: January 19, 2000
Appellant(s): DWORK ET AL.

John L. Rogitz
33,549
For Appellant

EXAMINER'S ANSWER

This is in response to the supplemental appeal brief filed 05/10/05 appealing from the Office action mailed 05/05/05

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. However the status of the claims has changed as follows:

Claims 1-5, 9-11, 12-18, 26-29, 31, and 33-35 are rejected.

Claims 6-8, 30, and 32 are objected.

Claims 19-25 are allowed.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

NEW GROUND(S) OF REJECTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-11 and 26-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-11 and 26-35 are directed to a computer-implemented method for digitally signing data. The examiner asserts that the collection of information does not fall within the statutory classes listed in 35 USC 101. Thus, while the claimed invention must be labeled as a device/method, it is in fact functional descriptive material (i.e computer program). Claims 1-11 and 26-35 are rejected as being directed to a functional descriptive material (i.e., computer program).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Goldenreich et al., "Public-Key Cryptosystems from Lattice Reduction Problems" MIT - Laboratory for Computer Science, November 12, 1996, pp 0-29

Whitfield Diffie and Martin Hellman, New Directions in Cryptography, IEEE 1976

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 12, and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by the paper by Goldreich et al.

As per claim 1, Goldreich discloses a signature scheme (page 3 paragraph 6) comprising: generating a lattice L having at least one short basis establishing a private key and at least one long basis establishing a public key (section 3.3); mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f" rendering infeasible the possibility of mapping two messages together in the space (section 1.2 page 3 paragraphs 5-6 "Our signature scheme"); and using the short basis, finding a lattice point of the lattice L that is close to the message point (page 18 section 5 especially section 5.1).

As per claim 2, the limitation of returning the message point x and the lattice point y as the digital signature, returning both the message point and the lattice point is necessary in order to verify the signature and further determine the authenticity of the message.

As per claim 12, the additional limitation of computer code for mapping a message or a concatenation thereof to a message point in n-dimensional space, the message point being a point of a grid or a point of an auxiliary lattice (page 10 section 3.3); computer readable code means for finding a point of a key lattice that is not the same as the auxiliary lattice (page 11 section

3.3.2); and computer readable code means for establishing a digital signature, based at least on the earlier mentioned points (page 18 section 5).

As per claim 26, the limitation of generating a lattice having at least one short basis and at least one long basis disclosed in Goldreich page 8, section 3.1 "Generate." A mapping that maps at least the message to a message point in n-dimensional space, the message point x being an element of a set spaced points not on the lattice (page 18 section 5.1 "Signature"). The limitation of using the short basis to find a lattice point in the lattice that is within a predetermined distance of the message point (page 18 section 5.1 "signature").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-5, 9-10, 13-18, 27-29, 31, 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldreich in view of Diffie/Hellman.

As per claim 3, further comprising randomizing the function f. Diffie/Hellman note (page 36, column 2, second paragraph) that a one way function f is a building function to both encryption functions (e.g. block ciphers) and key generators (pseudorandom sequence).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have continually changed the function f in a random fashion, because all pseudorandom sequences have periods from which the function f can be determined. One of ordinary skill in the art would have been motivated to do this because randomly changing this function permits the use of this function over a lengthy period of time without compromising the cryptosystem

As per claims 4 and 28, the limitation that the message f is randomized by concatenating the message u with a random number p. Diffie/Hellman note (last paragraph, column 2) that cipher text only attacks succeed because the cryptanalysis knows the statistical properties of a language or certain probable words or more generally certain message formats (called cribs) that enable the cryptanalysis to establish certain correspondence between cipher text and plaintext. The use of nulls, as it was known in the nineteenth century or padding or salting (especially for passwords), adds random text to the message to prevent such attacks from working.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have padded messages with random text (numbers). One of ordinary skill in the art would have been motivated to do this because to prevent the earlier mentioned attacks.

As per claims 5 and 29, the limitation that the function f maps the message u to a point on a grid disclosed by Diffie/Hellman page 35, column 2 paragraph 2. Diffie/Hellman disclose for the functions suitable for f sparse polynomials over finite field. Thus f maps u to a point in the range space of f. Both the domain and range spaces would constitute a finite grid and hence the limitation is met. Claim 5 is rejected.

As per claim 31, the limitation that the collision intractability of is based on a computational hard problem such as a lattice problem, Diffie/Hellman have pointed out that the one way function f are based on overwhelmingly difficult (hard) problems (see column 1 bottom page 35, Diffie/Hellman explain what they mean by overwhelmingly difficult in section 6 in terms of NP complexity) and Goldreich teach lattice problems as computationally hard for computing the digital signature.

Thus one of ordinary skill in the art at the time the invention was made would have been motivated to apply the teachings of Diffie/Hellman to the invention disclosed by Goldreich because the encryption system already has the lattice problem in place either in software or hardware or both.

As per claims 9 and 33, the limitation that the function f maps the message u to an auxiliary lattice. Diffie/Hellman disclose that the hard over which the Encryption function (i.e. hard lattice problem disclosed by Goldreich) does not have to be the same in which the function f is based (that is sparse polynomials over a finite field Diffie/Hellman page 35 second comment see Purdy comment), and thus one of ordinary skill in the art at the time the invention was made would have not necessarily been motivated to base both the encryption function and the hashing function on the same hard problem (that is the same lattice or different lattice problems) for security reasons. One might leak more information (bits) in the hashing process than in the encryption process or vice versus and thus might have to use different lattices or even different lattice problems, entirely.

As per claims 10 and 34, the limitation of verifying the digital signature by determining whether the distance between the lattice point x and y vary no more than a predetermine amount. Goldreich teaches the closest vector problem wherein when given a basis for a lattice, the task is to find the vector that is closest to v (page 6 section 2.1).

As per claim 35 that the predetermined distance is related to the number of dimensions n in the lattice, see Goldreich page 10 section 3.3.1.

Claims 13-15 and 17-18 with the limitation addressed above, are directed towards a computer program storage device with instructions to implement the method claims 1, 6, 3, 4 and 8-9, and are therefore rejected in view of the same prior art of record.

As per claim 16, the limitation that f maps the message to a point on a grid was addressed in 5, the limitation of collision intractable was addressed in claim 6 and finally the intractability being based on the hardness of the lattice problem was address in claim 7. It would have been obvious for one of ordinary skill in the art at the time the invention was made to have been motivated to combine these features because they each add to the overall security and ease of implementation of the encryption device.

As per claim 27, the limitation that the mapping is undertaken using a function f is met as a mathematical truism. For example see the CRC Concise Encyclopedia of Mathematics by Eric W. Weissten page 1136. The terms FUNCTION and MAPPING are synonymous with map. Even if this were not considered Goldreich as modified by Diffie/Hellman disclose that the mapping process is via a one way function f which in from the standpoint of Diffie/Hellman is necessary in order to determine data integrity (page 35 second column), authenticity (page 35 second column) and data security (privacy page 30, bottom and continuing to the second column).

(10) Response to Argument

In response to the appellant's arguments regarding the primary reference does not teach using a function that renders infeasible the possibility of mapping two messages close together (7a). The examiner would like to begin by describing how the examiner interpreted the claims and how it affects the reading of the Goldreich reference.

The claim preamble of claims 1 and 12 use the transition "comprising," which is inclusive or open-ended and does not exclude additional, unrecited elements or method steps. As a result, when the Goldreich reference includes the "additional step of pre map hash" as disclosed in the appellant's arguments (appeal page 3 lines 11-15). The appellant does not claim rendering infeasible the possibility of mapping two messages close (emphasis added) together. The claim recites "...rendering infeasible the possibility of mapping two messages together in the space."

The system of Goldreich teaches Public-Key Cryptosystems is from Lattice reduction problems. As disclosed by the appellant, Goldreich does envision that close mapping and therefore mapping together of a message (7a page 3). However, rather than teach away from mapping function that always renders such feasible Goldreich teaches the method to overcome mapping two messages together (section 5.2). This method is the pre map step mentioned in the appellant's arguments. The added step makes it infeasible for the mapping function of Goldreich to map two messages together. Since the claim uses the "comprising" transitional phrase it is acceptable to include this added step of pre mapping.

The appellant argues that the reference explicitly envisions that close mapping is sometimes desirable and is therefore teaching away from a mapping function that always renders such infeasible (7a page 3). This is not found persuasive. The reference discloses (page 3 section 1 Out signature scheme). One embodiment wherein "applying the method in a setting where this property is desirable (e.g. signing analog signals which may change a little in time)." However, the reference also discloses an embodiment wherein "applying the method to a message space where such property (lattice point which is close)" is undesirable. The undesirable specifies the embodiment of claim 1 and claim 26 wherein mapping together is made infeasible. This is made possible by adding the pre hash. The first embodiment does not teach the appellant's application, however the second embodiment wherein the property is undesirable is the embodiment that teaches the appellant's application.

In reference to the argument about claims that recite in part finding a point "y" of a key lattice £ that is not the same as the auxiliary lattice on which the message point x is located (7a page 4). Thus the appellant argued that the message point "x" being an element of a set of spaced-apart points that are not on the lattice. However, a closer examination of the claims shows that the claim recites "the message point "x" being a point of a grid or (emphasis added) a point of an auxiliary lattice." Since the point may be of a grid or a point that is not on the same lattice. The claim does not include only points that are on the auxiliary lattice. Goldreich teaches a point that in on the same lattice that uses the grid therefore teaches the limitation.

Appellants arguments (7b) in reference to claims 6-8, 11, 30, and 32 are found persuasive and therefore claims 6-8, 30, and 32 are objected. Claim 11 is rejected as shown in the new grounds of rejection above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

Paula W Klimach

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

Conferees:

Kim Vu

Kambiz Zand

PETER WONG, DIRECTOR
TECHNOLOGY CENTER 2100